GOUVERNEMENT

Liberté
Égalité
Fraternité

Pôle d'expertise de la régulation numérique

Éclairage sur...

Applications mobiles : quels enjeux de sécurité pour leur distribution hors des magasins des OS ?

La démocratisation des smartphones s'est accompagnée de changements radicaux sur la manière d'installer nos applications. D'un modèle décentralisé et ouvert, avec des téléchargements depuis des sites tiers sur nos ordinateurs, nous sommes passés sur nos smartphones à un modèle centralisé et parfois fermé, où l'installation d'applications se fait souvent, et dans certains cas exclusivement, depuis le magasin d'applications du développeur du système d'exploitation.

Ce mode de diffusion restreint est aujourd'hui remis en cause par plusieurs règlements nationaux ou internationaux en préparation, dont le *Digital Market Act*, qui visent à ouvrir la diffusion d'applications à des sources tierces. Cette ouverture souvent justifiée par des enjeux économiques, soulève cependant des enjeux liés à la protection de l'utilisateur. Cet éclairage présente les problématiques techniques liées à ces questions de sécurité.

Février
2022
.02

La problématique de la diffusion d'applications sur les systèmes d'exploitation mobiles est la suivante : d'un côté les développeurs de systèmes d'exploitation privilégient une diffusion des applications via des magasins d'applications exclusifs, pour protéger l'utilisateur des applications malveillantes, qui pourraient compromettre la sécurité du matériel ou de l'utilisateur. De l'autre côté, les éditeurs d'applications légitimes préféreraient ne pas être contraints par les politiques tarifaires ou éditoriales des magasins d'applications exclusifs et souhaiteraient donc plus de concurrence dans ce domaine avec parfois la possibilité de distribuer directement eux-mêmes leurs applications. Enfin, il faut pouvoir offrir à l'utilisateur à la fois la meilleure protection contre les logiciels malveillants, et à la fois le plus de choix et des conditions tarifaires concurrentielles pour les applications qu'il pourrait télécharger.

QUE SONT LES LOGICIELS MALVEILLANTS ?

Un logiciel malveillant est un logiciel conçu dans le but de nuire à un système informatique ou à ses utilisateurs. Dans certains cas ces logiciels peuvent exploiter des vulnérabilités logicielles ou matérielles afin d'accéder à des ressources privilégiées ou privées et compromettre ainsi l'intégrité du système. Dans d'autres cas, ces logiciels peuvent avoir un comportement malveillant même sans utiliser de vulnérabilités (affichage de publicités intempestives, enregistreur de frappe, vol de données personnelles…). Dans ce cas ils peuvent nuire à l'utilisateur, mais n'affectent pas l'intégrité du système.

COMMENT SE DIFFUSENT LES LOGICIELS MALVEILLANTS ?

Même si certains logiciels malveillants peuvent s'installer sans actions de la part de l'utilisateur, dans la majorité des cas l'installation s'effectue sur l'initiative de l'utilisateur. Pour inciter l'utilisateur à l'installer, une application malveillante peut, par exemple, se faire passer pour une application légitime, et effectuer des actions malveillantes à l'insu de l'utilisateur. Il arrive aussi qu'une application légitime devienne malveillante, par exemple à la suite d'un piratage de l'éditeur de l'application ou encore si l'éditeur utilise sans le savoir une brique logicielle malveillante.

QUELLES PROTECTIONS EXISTENT CONTRE CES LOGICIELS ?

Il convient ici de distinguer deux types de protection :

- Les protections apportées par le système d'exploitation.
- Les protections apportées par un audit pré-installation.

Protections apportées par le système d'exploitation

Le système d'exploitation est un logiciel central dont le rôle est d'assurer notamment la liaison entre les applications et le matériel, de gérer la répartition des ressources disponibles entre les différentes applications, mais aussi d'assurer la protection de l'utilisateur et du matériel contre les logiciels malveillants. Pour cela il dispose de plusieurs outils :

- L'**isolation des applications** et le **système de permissions** qui permettent de restreindre à une application l'accès aux données d'autres applications ou aux fonctions du système. Pour accéder à ces données ou à ces fonctions, l'application doit alors demander la permission au système d'exploitation, qui s'accompagne, la plupart du temps, d'une notification à l'utilisateur qui peut alors accepter ou refuser cette demande. Le système de permissions donne une visibilité importante à l'utilisateur sur le comportement de l'application. Par exemple, il serait anormal qu'une application de lampe torche demande l'accès au carnet d'adresses.
- L'**utilisation d'interfaces de programmation pour accéder aux fonctionnalités du système**. Dans un système d'exploitation moderne, les applications ne peuvent communiquer directement avec le matériel. Elles ne peuvent accéder qu'à des fonctionnalités spécifiques du matériel, exploitées par le système d'exploitation, et mises à disposition via des interfaces de programmation. C'est ainsi le système d'exploitation qui se charge de la communication directe avec le matériel et qui transmet les résultats de cette communication à l'application. Ce système d'isolation du matériel au travers d'interfaces restreintes permet de diminuer considérablement la surface d'attaque des logiciels malveillants, qui ne peuvent interagir qu'avec ces interfaces ne donnant accès qu'à des fonctionnalités limitées et présentant une sécurité renforcée.
- La **détection à l'exécution de programmes ou comportements malveillants**, par exemple via l'analyse de l'empreinte numérique[1] d'une application ou d'une partie d'une application pour la comparer à une base d'empreintes numériques de logiciels malveillants, **à la manière d'un antivirus**. Cette technique permet de détecter et de bloquer des logiciels malveillants même après leur installation.

[1] L'empreinte numérique d'une application est une suite de caractères alphanumériques construite pour être unique pour une application donnée ou une partie de celle-ci. Deux applications qui auront la même empreinte seront donc, de manière quasi-certaine, parfaitement identiques.

Le système d'exploitation apporte donc déjà des protections contre les logiciels malveillants, autant d'un point de vue de la protection du matériel que de l'utilisateur. De plus, il convient de noter que **tant qu'aucune vulnérabilité n'existe au sein du système d'exploitation, il est impossible pour une application de compromettre le matériel ou le système d'exploitation** lui-même. En d'autres termes la sécurisation du matériel et du système d'exploitation repose exclusivement sur les développeurs du système d'exploitation et jamais sur les développeurs d'applications.

Les protections du système d'exploitation ne sont réellement efficaces que si les utilisateurs disposent d'un système à jour sur leurs appareils, qui leur permet de bénéficier des correctifs de sécurité, de raffinements sur le système de permissions, de traçabilité du comportement des applications, de systèmes de protection des données personnelles, etc.

Protections apportées par un système d'audit pré-installation

Un **système d'audit des applications**, avant l'installation par l'utilisateur, **apporte une protection supplémentaire** contre les applications frauduleuses en analysant et en comparant la description des applications et leurs comportements réels. Ainsi, l'auditeur de l'application agit comme un tiers de confiance pour l'utilisateur qui souhaite installer des applications légitimes.

Les protections apportées par un tel système d'audit ne sont efficaces que si les audits sont poussés. En effet, un audit superficiel qui se contente de comparer la description d'une application et son aspect visuel au lancement ne peut découvrir que des applications grossièrement malicieuses. Un audit efficace doit également vérifier les permissions de l'application, les fonctions du système auxquelles elle accède, les échanges de données avec l'extérieur, les politiques de traitement des données en dehors de l'application, etc.

L'audit pré-installation peut parfois s'appuyer sur l'analyse du code source, et garantir que l'application installée correspond à ce code, mais cette situation est rare, et aucun des grands développeurs de systèmes d'exploitation ne fait de vérification du code source des applications tierces qu'ils auditent et distribuent dans leurs magasins d'applications.

Un audit de pré-installation ne peut enfin vérifier que le comportement local de l'application, et ne pourrait pas par exemple détecter le comportement malveillant d'un développeur dont l'application de carnet d'adresses sauvegarderait les contacts sur son serveur, puis aurait une utilisation malveillante de ces données personnelles stockées sur son serveur (dissémination des contacts depuis le serveur par exemple).

COMMENT ASSURER LA SÉCURITE DES UTILISATEURS TOUT EN OUVRANT LA DIFFUSION AUX TIERS ?

La diffusion d'applications sur nos smartphones peut être réalisée sur un modèle plus ouvert et décentralisé sans remettre en jeu le niveau de sécurité des utilisateurs conféré par les pratiques présentées comme l'état de l'art en la matière, voire en l'améliorant. En effet, nous avons vu que le système d'exploitation est au cœur des protections contre les logiciels malveillants, à la fois contre les applications tentant de nuire au système ou au matériel, mais aussi contre les applications frauduleuses qui cherchent à nuire à l'utilisateur. Pour renforcer la sécurité de l'utilisateur, il est important de prendre des mesures au niveau du système d'exploitation :

- Concevoir un **système de permissions à grains fins**, qui permet une vraie traçabilité de comportement des applications, et limite la surface d'attaque des logiciels malveillants.
- Mettre en place des **systèmes de détection de codes malveillants**, qui peuvent permettre de stopper la diffusion de logiciels malveillant, diffusés par des moyens tiers.
- Mettre en place des **moyens de vérification de certificats numériques**, qui permettent de certifier des applications, quels que soient leurs modes d'installation.
- Garantir un **suivi et un déploiement des mises à jour du système**, même sur les appareils anciens, afin que tous les utilisateurs puissent bénéficier des améliorations ou correctifs de sécurité sur leurs appareils.

Nous avons également vu que **ces protections peuvent être complémentés par un système d'audit des applications** avant même leur installation. **À l'heure actuelle ces audits sont réalisés au sein des magasins d'applications qui assurent également la distribution de celles-ci. Cependant, il est simple de décorréler ces deux processus**, grâce aux systèmes de certificats numériques, qui peuvent à la fois garantir qu'une application que l'on souhaite installer correspond strictement à une application qui a par ailleurs été auditée mais aussi que la description de l'application que l'on souhaite installer est strictement identique à celle soumise au processus d'audit. Le système d'exploitation peut alors vérifier le certificat d'une application lors de son installation ou son exécution. Ce certificat peut également être révoqué par le développeur de l'application, s'il estime que son application a été compromise, par l'auditeur s'il estime a posteriori que l'application n'aurait pas du être certifiée, ou même mis dans une liste noire par le développeur de système d'exploitation, s'il estime que l'application pose des problèmes majeurs à la sécurité de son système ou des utilisateurs.

Dans un tel schéma, l'audit peut être réalisé par exemple par les équipes du développeur du système d'exploitation, la charge étant compensée par une rémunération adéquate. Des tiers peuvent alors proposer la distribution des applications auditées et certifiées, y compris pour ce qui concerne leur description.

Ce travail d'audit peut très bien également être effectué directement par des magasins d'applications tiers, ou des organismes d'audits indépendants de la distribution**. Les vérifications faites à l'occasion des audits conduits par les magasins d'application actuels des développeurs de systèmes d'exploitation sont en effet toutes reproductibles par des tiers.**

Cependant il est nécessaire :

- D'encadrer les magasins d'applications, ou les organismes d'audits pour **répondre à un standard garantissant un certain niveau de revue des applications** proposées.
- D'assurer un **suivi dans le temps des applications auditées**, afin de pouvoir permettre la révocation de leurs certificats numériques et dans certains cas la suppression de l'application si un problème venait à être découvert après l'audit.

Dépôt légal : en cours
contact.peren@finances.gouv.fr

Service à compétence nationale, le Pôle d'expertise de la régulation numérique (PEReN) fournit, aux services de l'État et autorités administratives intervenant dans la régulation des plateformes numériques, une expertise et une assistance technique dans les domaines du traitement des données, des data sciences et des procédés algorithmiques. Il s'investit également dans des projets de recherche en science des données à caractère exploratoire ou scientifique.

PEReN – 120 rue de Bercy, 75572 Paris Cedex 12